NETWITNESS

netwitness.com

WHITEPAPER

Security and AI:

What's hype and what's real

Table of Contents

Executive Summary

How worrisome are the threats that artificial intelligence (AI) poses to enterprise security? Quite worrisome, in fact. But AI holds just as much promise – perhaps even more -- as a tool for cyber defense.

Threat intelligence research shows that malicious actors are already discussing how to use large language models (LLMs), also known as "generative AI" – the kind of AI that creates text, photos, video, and other forms of content – to break into organizational systems and networks.

But AI shows great potential for cyber defense, as well. Many threat research and cybersecurity companies have already been working with applied data science such as AI and machine learning for many years. We could even have a leg up on malicious actors.

From catching and correcting coding errors before launch to flagging unusual behaviors in real time to block breach attempts, AI stands at least as great a chance of protecting business as it does of disrupting it.

In this paper, we'll examine the hype around AI, explore ways the technology might be used to carry out cyberattacks, and discuss its exciting potential for detecting and responding to intrusions and atttempts more rapidly and effectively than ever before.

Why AI is suddenly top-of-mind

Big Tech is investing big in AI: Google, Microsoft, Facebook, IBM and others have already invested what amounts to billions of dollars in research, development, and use of the technology[1] to

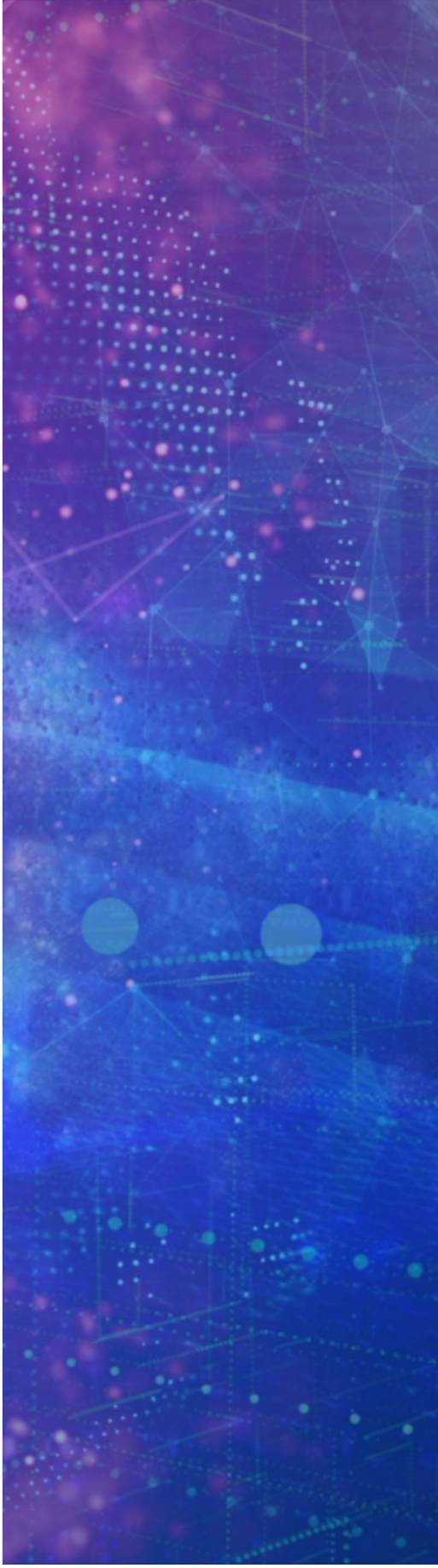
- Quickly analyze the massive amounts of data their systems collect
- Distribute and deliver customer orders
- Automate tasks
- Increase worker productivity
- Improve voice assistants
- Enhance customer service

And much more.

The technology is not cheap.[2] Often, it must be trained to perform its given task, a time-consuming and expensive endeavor. The hardware is costly, as well. And to stay apace with, or ahead of, competitors, enterprises are investing heavily in AI research.

At the same time, the hardware has vastly improved, creating ideal conditions for the rapid advances we are seeing now. Processing complex information at the speed of thought requires massive CPUs and GPUs,[3] and chip manufacturers are delivering. Some are even producing dedicated AI processors called Vision Processing Units, or VPUs.[4]

The combination – capital for research and development and training plus strides in compute power enabling speed-of-thought processing – is ushering in either a golden digital age or a Pandora's Box unleashing forces into the world that we'll never be able to control. Which is it? Most likely, the answer lies somewhere in between.



1. exoinsight, "How Much Is Invested in Artificial Intelligence?" https://insight.openexo.com/how-much-is-invested-in-artificial-intelligence/
2. CNBC, "ChatGPT and generative AI are booming, but the costs can be extraordinary," https://www.cnbc.com/2023/03/13/chatgpt-and-generative-ai-are-booming-but-at-a-very-expensive-price.html
3. SiliconANGLE, "Generative AI drives an explosion in compute: The looming need for sustainable AI," https://siliconangle.com/2023/02/05/generative-ai-drives-explosion-compute-looming-need-sustainable-ai/
4. digitaltrends, "Intel thinks your next CPU needs an AI processor — here's why," https://www.digitaltrends.com/computing/intel-meteor-lake-vpu-computex-2023/

Friend, foe, or both?

Technology geeks and business executives are far from the only ones excited about an AI-powered future. Artificial intelligence – a term coined in the 1950s – has long captured the popular imagination. And we've been using it for more than a decade.

AI already vacuums our floors. It answers our questions, plays the music we request, makes dinner reservations on our behalf, and more via voice assistants such as Alexa and Google Home.

Soon, it could drive our cars so we don't have to. It would be critical to the immersive "metaverse" envisioned for the future. It could connect and orchestrate the workings of our cities and our homes far beyond what we experience today, taking much of the hassle and stress out of daily life. It could ensure that our refrigerators never run out of milk – or beer.

Business executives may hope to use AI to do the jobs they can't find qualified people to fill. AI might let them run their factories with little or no human intervention. It could aid and speed software production. There's even speculation that AI could alert developers to coding errors even as they write, and prescribe or automatically apply fixes[5] – a cybersecurity win, as bad code is a top application cybersecurity vulnerability.[6]

5. Forbes, "Generative AI: Cybersecurity Friend and Foe," https://www.forbes.com/sites/heatherwishartsmith/2023/06/06/generative-ai-cybersecurity-friend-and-foe/?sh=99da5284bd2d
6. Security Boulevard, "8 Most Commons Causes of a Data Breach," https://securityboulevard.com/2022/07/8-most-common-causes-of-a-data-breach/

To err is (in)human

But AI comes with risks, as well. An organization's AI models will work only as well as the data used to train them. Erroneous data will cause AI to make mistakes – perhaps damaging ones. If it is responding automatically, errors might not be caught in time. There are no magic beans; there is no silver bullet: there are only, in the end, technologies designed by humans, who invariably err.

Where there's a vulnerability, so shall we find malicious actors, whose numbers and motives are multiplying.[7] Not only are they likely to use AI to find their way into organizational systems and networks, they will certainly target AI-powered software wherever they find weaknesses. Here are just a few ways they might attack:

- **Tricking machine learning models. Threat** actors can use a technique known as "adversarial machine learning" or "adversarial AI" to trick machine learning models into doing their bidding.[8] For example, they might tell the model to create a backdoor into the system by which they can enter undetected.
- **Automating attacks.** This already happens with botnets and other automated attack types[9]. Using AI, bad actors can attack their targets continuously, increasing the likelihood that they will slip in.
- **Creating mutating malware.** Threat actors may use LLMs to create malicious code that changes[10] with every application programming interface (API) call, making it harder for cybersecurity software to detect their exploits.
- **Finding and exploiting vulnerabilities in open-source software libraries.**

AI to the rescue? Some challenges.

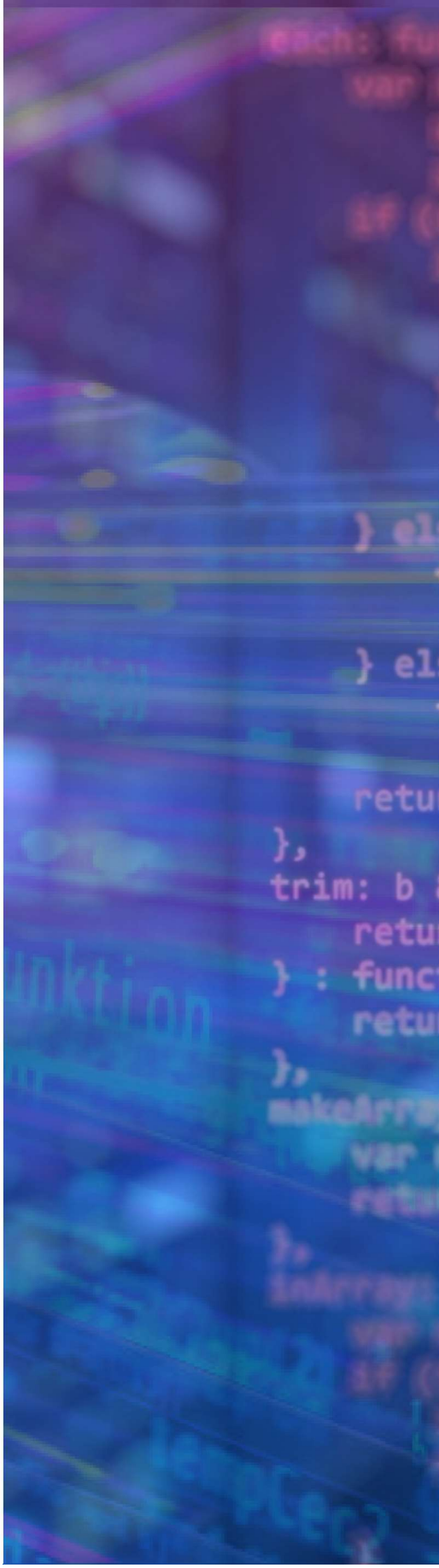
It's not a popular term, but "arms race" fittingly describes the AI cybersecurity scene right now. Every company researching and developing AI defense is racing to be first with effective security tools. And all together, the industry as a whole is working around the clock to divine not only how adversaries might use AI for nefarious purposes, but also how to stop them.

7. Security Intelligence, "A Perfect Storm: 7 Reasons Global Attacks Will Soar in 2023," https://securityintelligence.com/articles/7-reasons-global-attacks-will-soar-2023/
8. NIST National Cybersecurity Center of Excellence, "Artificial Intelligence: Adversarial Machine Learning," https://www.nccoe.nist.gov/ai/adversarial-machine-learning
9. OWASP, "OWASP Automated Threats to Web Applications," https://owasp.org/www-project-automated-threats-to-web-applications/
10. CSO Online, "ChatGPT creates mutating malware that evades detection by EDR," https://www.csoonline.com/article/575487/chatgpt-creates-mutating-malware-that-evades-detection-by-edr.html

For every AI-powered attack tool that threat actors may use has, or will have, exists a counterpoint in cyber defense that also uses AI. Many defense capabilities already exist, and are ready and waiting to be called to action. Others are in the works.

Securing AI and using it in cybersecurity is far from easy. We in the business face a number of challenges,[11] as this list from the European Union Agency for Cybersecurity (ENISA) shows:

- Achieving optimal accuracy under real-world conditions and not in a simulated environment;
- The need for computational complexity and 'low-latency operation' to be addressed, especially when the system being monitored is of critical importance;
- The need to investigate whether the inferred models are valid or biased, or whether there are perceive changes in the time variance;
- Ensuring that the security of the protection mechanism is assessed following a standardized framework that considers diverse malicious attempts, cases, figures of merit, etc. (security-by-design);
- Preserving privacy: protecting training data and confidentiality of the information flowing in the system



11. ENISA, "Artificial Intelligence and Cybersecurity Research," https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research

Experience matters

At NetWitness, we've been speaking AI for more than a decade. Our unique approach brings data scientists, computer scientists, threat intelligence specialists, and AI security researchers together to collaborate and innovate potent, cutting-edge uses for AI in our threat detection, investigation, and response solutions.

As our record demonstrates, NetWitness is uniquely positioned among cybersecurity vendors by virtue of our deep understanding of forensics and our software's ability to process and analyze massive amounts of data – the fuel that drives artificial intelligence – on the network as well as in systems incident and event management (SIEM) logs.

Mission-oriented, we at NetWitness are moving ahead with applying advanced AI capabilities to our products that enable our customers to protect themselves. We aim to provide our customers with the highest degree of

- Understanding of their environments and the risks and threats to them
- Transparent visibility into all their digital assets and their security status
- Real-time threat (and threat actor) detection
- Proactive threat intelligence for readiness and resilience
- Real-time, automated responses to active threats and actors

A historic moment

Never in human history have we stood at this particular crossroads, where AI and cybersecurity intersect and point to a horizon filled with unknowns – which include possibilities. Artificial intelligence brings a plethora of exciting benefits, actual and possible, to the workplace and society, as well as challenges galore for cybersecurity.

The good news is that, having immersed ourselves in AI algorithms for more than a decade and collected mountains of data, NetWitness has a leg-up on threat actors. Our renowned suite of security products provides maximum protection against adversaries, no matter what technology they are using. To learn more about our products and projects – AI-driven and not – contact NetWitness today.